数理解析研究所講究録 1256 巻 2002 年 71-88

ワーリング問題について — 低次の場合を中心に

岩手大学 教育学部　川田 浩一 (Koichi KAWADA)
Faculty of Education, Iwate University

1. 序

今回の研究集会の講演者のうち、私が最年長であったと思いますが、年齢の点で発表をする資格がなかったんではないか、と恐縮しております。もはや「若手」と呼んでいただける時期を過ぎているのかもしれませんが*、にもかかわらずこの特別な趣向の研究発表会に参加させていただけて、喜んでおります。会を主催してくださった伊原康隆先生ならびに関係された方々、またご推薦くださった明治学院大学の村田玲音先生に、厚く御礼申し上げます。

自分の考えていることについて1時間も話をさせていただける、というのはめったにないことですから、楽しみに思いながらも重圧を感じる面もありましたが、とにかく人様に興味をもって聞いていただけるだけのものにしたい、と意気込んであれこれと考えを巡らせておりました。結局研究集会の始まる12月19日になってもどう話そうか迷う部分も残り、行きの新幹線や京都の地下鉄の中でも考え事をしながらぼんやりと過ごしておりました。その日は数理解析研究所に行く前にとりあえず宿に荷物を置いていこうと思い、予約したホテルに寄ってフロントの人に「荷物を預かってください。」と言ったところ..... ただ一つの荷物が、背中にしょっているべきリュックサックが、ない。手ぶらの男に荷物を預かってくれと言われたホテルマンも驚いたろうが、こっちだってなかなか恥ずかしい。とっさに「なーんちゃって。」とか言って走って逃げる、という非常手段が頭をよぎったが、なにぶんそれから3泊するつもりだったから、旅の恥はかき捨て、とはいかない。ジャンパーを脱いで預けてその場を取り繕う、というアイディアも浮かんだが、人は着ているジャンパーを「荷物」と言うだろうか、という点が気になり踏み切れなかった。結

*若手ではないが岩手に住んでます、というのは字としては駄洒落になっていると思いますが、つまんないですか?

局「あれぇー、どぉこやっちゃったかなー。」とつぶやきながら背を向けて立ち去る、という平凡だがかなりみっともない行動に終わった。

そのフロント係の人とまた顔を合わせるのか、というのもつらかったが、もちろんそれは二の次で、まずは荷物である。帰りの新幹線の切符も打ちかけの論文の原稿の入ったコンピューターもその中なのだ。この見知らぬ街でもし見つからなかったら、と思うとめまいがした。とにかく何か思い出さねば、とその一点に集中し、私の頭脳は近年まれにみるスピードで回転した。言うまでもないことだが、翌日の自分の発表をどうするか、なんてことは既に頭の中から消去されていた。京都駅を出るときは切符を出したりしたからリュックを持っていたことは確実である。そのあとそれを手放しそうなところといえば地下鉄の中くらいだ、たぶん無意識のうちに網棚の上にでも置いてしまったんだろう、と考え、四条駅に戻って駅員さんにたずねてみた。するとまず、何時何分発のどこ行きの電車の前から何両目のどのあたりに置き忘れたのか、というようなことを聞かれた。この質問にちゃんと答えられる場合、置き忘れたというより、計画的に放置した、というほうが日本語として正しい気もする。とはいえ係りの方はさすが専門家である、新幹線の到着時刻や通った改札や階段の情報を基に推理し、何個所かに電話をして調べてくださった。しばらく待つことになったが、この間はとても心細かったものである。5分ほどして、いや本当はもっと短かったのかもしれないが、国際会館駅にそれらしいものがあるという連絡があり、行ってみると確かに自分のもので、本当にほっとした。四条駅に戻ってお世話になった駅員さんには丁重にお礼を申し上げたが、この場でももう一度発見に関係してくださった京都の地下鉄職員の皆様に、ご迷惑をお掛けしたことをお詫びし、ご尽力に深い感謝の意を表したい。

そんなこんなで結局は大事には至らずに済んだが、昼飯を食う時間は失った。開会の時間ぎりぎりに数理解析研究所に着いたものの、頭の中は、夕飯こそうまいもんをいっぱい食ってやる、ということでいっぱいであった。

そろそろ、こいつは講究録というものを誤解してるんじゃないかとご心配の、あるいはお怒りの、読者もいらっしゃると思うので、エッセイはいいかげんこのへんで終わりにして、次節からは私の話の内容をもう一度整理し直して記させていただくことにする。なお、以下に現れる参考文献のうち本文末に明記されていないものについては、Nathanson [6] や Vaughan [9] の Bibliography をご参照いただきたい。

2. Waring 問題—$g(k)$ と $G(k)$

すべての自然数は高々4個の平方数の和で表せることをLagrangeが1770年に証明したことをうけて、Waringは同年、すべての自然数は高々9個の立方数の和、高々19個の4乗数の和、などと表すことができる、と証明なしで記した。これが発端となって自然数をべき乗数の和として表すことに関する様々な問題が研究されるようになり、そのような問題を総称して現在ではWaring問題といっているようである。

以後 k は2以上の自然数とし、単に k 乗数といったら自然数の k 乗を指すものと約束しておこう。上でも、高々9個の立方数、と書いたが、これも"正の"立方数を意味している。この約束はWaring問題に関しては通例である。因みに実際の講演の際には0も k 乗数に含めることとしておいたのだが、これはあのときはそうした方が板書が簡潔になる部分があったからである。0を k 乗数に入れるかどうかはWaring問題においては全く本質的な問題ではなく、例えば「高々9個の」などと言う際の「高々」を省いてもよいかどうか、という程度のことである。ただし"負の"k 乗数をも含めて考える場合は状況が違ってくるところがある。例えば任意の整数 n に対して $m = (n^3 - n)/6$ とおけば m も整数で、

$$n = n^3 - 6m = n^3 + (1-m)^3 + (-1-m)^3 + m^3 + m^3$$

だから、任意の整数は高々5個の"正または負の"立方数の和となることがすぐ分かったりする。このように負の k 乗数を含める場合については、例えばNathanson [6] の§4.3、Easier Waring's problem の節を参照されたい。

Waring問題においても多様な研究課題あるいは問題意識があるが、その究極の目標の一つは、自然数 s と k に対し、高々 s 個の k 乗数の和で表せる自然数、表せない自然数をすべて決定する、ということだといえよう。この意味では $k=2$ の場合、つまり平方数の場合は既に終わっている。実際この節の冒頭で触れたLagrangeの四平方数定理がある上、高々3個の平方数の和で表せない自然数は $4^r(8m+7)$ (r, m は0以上の整数)の形のものに限ることが知られているし、さらに自然数の素因数分解の形をもってそれが2個の平方数の和となるかどうかを判定できることもよく知られているところであろう。$k \geq 3$ の場合はこの意味での最終的な結果から程遠いことしか分かっていない。そこで次のように定義される $g(k)$ および $G(k)$ の値を調べることがとりあえずの目標となる。

$g(k)$: 「すべての自然数が高々 s 個の k 乗数の和で表せる」ような s の最小値

$G(k)$: 「十分大きい自然数はすべて高々 s 個の k 乗数の和で表せる」ような s の最小値

このように定義を書くのが普通なのだが、もしかしたら他の分野の方には次のような定義の書き方のほうがしっくりするかもしれない。まず自然数 n, k に対し、$n = x_1^k + \cdots + x_s^k$ となる自然数 $x_1, \ldots, x_s$ が存在するような s の最小値を $s(n,k)$ とでもしよう。少なくとも $s = n$ のときはそのような x_j 達は存在する (全部 1 とすれば良い) から、各 n, k に対しそのような $s(n,k)$ は確定する。さらに自然数全体の集合を $\mathbb{N}$ で表すとすれば、

$$g(k) = \max_{n \in \mathbb{N}} s(n,k), \qquad G(k) = \limsup_{n \in \mathbb{N}} s(n,k)$$

である。もちろん任意の k に対して $g(k)$ が存在すること (有限であること) はそれほど自明なことではなく、それを証明することをもともとは「Waring の問題」といっていたようである。それが初めて証明されたのは 1909 年のことで、Hilbert による。

さて、実数 z の整数部分を $[z]$ で表すことにし、$n_k = 2^k[(3/2)^k] - 1$ とおくと、$n_k < 3^k$ だから、n_k をできるだけ少ない個数の k 乗数の和で表そうとすると、$([(3/2)^k] - 1)$ 個の 2 の k 乗と $(2^k - 1)$ 個の 1 の k 乗の和で表すしかないから、$s(n_k, k) = 2^k + [(3/2)^k] - 2$ であることが分かり、よって

$$g(k) \geq 2^k + [(3/2)^k] - 2 \tag{1}$$

を得る。とくに $g(3) \geq 9$、$g(4) \geq 19$ だから、この節の初めに紹介した Waring の記述により、彼は $g(3) = 9$、$g(4) = 19$ と予想した、といって良い。

実は次節で述べる通り現在では各 k に対して $g(k)$ の値は決定されている。その歴史についても後で触れるが、最後まで残ったのは 4 乗数の場合で、$g(4) = 19$ の証明が完全に発表されたのは 1993 年のことであるから、そんなに昔のことではない。だが $g(k)$ の決定はもっとずっと前に本質的には終わっていた、ともいえる。例えば 1925 年に Hardy-Littlewood は $G(4) \leq 19$ を示していて、その証明によれば、C より大きいすべての n に対して $s(n,4) \leq 19$ となるような C が原理的に計算可能となる。その

C を計算し、それ以下のすべての自然数 n について $s(n,4)$ を求めることは、有限回の単純計算を繰り返すことで可能となる。先に注意したように $s(79,4)=19$ だから、すると $\max\{C,79\}$ 以下の n に対する $s(n,4)$ の最大値として $g(4)$ の値が決まる。それが本当に 19 になるかどうかは別問題だが、この意味で Hardy-Littlewood が $G(4) \leq 19$ を証明した瞬間に $g(4)$ は原理的には決定できていたわけである。とはいえ Hardy-Littlewood の議論によって得られるこの C は大きすぎて、それ以下のすべての n について $s(n,4) \leq 19$ であることを確認することは現在の最新の大型コンピューターをもってしても現実には不可能、というべきである。この状況はその後の Hua(華羅庚) や Davenport らのより進んだ研究を用いても同様で、例えば 1940 年に Auluck が得た上述の C の値は $e^{e^{204}}$ である。これは俗に天文学的数字といわれるような数と比べものにならないほど大きい。この C のような値を現実にコンピューターが届く程度の大きさにまでおとすことは、いろいろな数学的アイディアや工夫を要する仕事であった。

ちょっと深入りしすぎたが、いずれにしても、ここに述べたような意味で、それぞれの k に対して $g(k)$ を求めることは、1920 年代半ばにして既に理論的には可能であった、といえる。

また前出の $G(4) \leq 19$ の例のように、少なくともこれまでのところは、$G(k) \leq s$ という形の評価の証明は、「ある原理的に計算可能な定数 C があって、C より大きい自然数はすべて (ちょうど)s 個の k 乗数の和で表せる」というほんのちょっとだけ強い命題の証明になっている。したがって $G(k) \leq s$ が示されるということは、実際、s 個の k 乗数の和で表せない自然数を原理的にはすべて求めることができる、ということを意味することになる。こういう $G(k)$ に関する研究は 1920 年頃に Hardy、Littlewood、Ramanujan らが circle method を創始してから大きく進展し、それ以来、以上のような事情により、$G(k)$ を上から評価することが Waring 問題における中心的な研究課題となっているのである。

発表の後で、この $G(k)$ に関する予想について、Hasse の原理あるいは local-global principle と関連付けて述べてみたのだが、やや明確でなかったかもしれない。そこで、話の本筋とは関係ないが、Hardy-Littlewood によるその予想をここではっきりさせておこう。「すべての自然数 q, n に対して合同式

$$x_1^k + \cdots + x_s^k \equiv n \pmod q$$

が、x_1 が q と互いに素であるような整数解 $x_1, \ldots, x_s$ をもつ」ような s の

最小値を $\Gamma_0(k)$ とすると、$k \geq 3$ に対して†

$$G(k) = \max\{k+1,\ \Gamma_0(k)\} \tag{2}$$

と予想されている。少なくとも $G(k) \geq \max\{k+1,\ \Gamma_0(k)\}$ であることは容易に分かる (Vaughan [9], §2.8, Exercise 2)。k が与えられれば $\Gamma_0(k)$ を計算することは初等的な作業であり、これについては Vaughan [9] の §2.6, §4.5 および §4.6 の Exercise 3 などを参照されたい。$k \geq 3$ のとき、k が 2 のべきなら $\Gamma_0(k) = 4k$、そうでなければ $\Gamma_0(k) \leq 3k/2$、といったことが例えば知られている。よって上の予想(2) によれば、すべての k に対して $G(k) \leq 4k$ であり、k が 2 より大きい 2 のべき乗ならその等号が成立する、と予想される。

$G(k)$ に関して証明されている結果については、$k = 3, 4, 5$ の場合はそれぞれ後の第 $(k+1)$ 節の中で触れる。大きい k については、Wooley [15] による評価 $G(k) \leq k(\log k + \log\log k + 2 + O(\log k/\log\log k))$ が最良である。ここではこれ以上は記さないが、$5 \leq k \leq 20$ なる k については、$G(k)$ に対する現在最良の評価は Vaughan-Wooley [10], [11], [12], [13] により得られているので、興味のある方はそれらをご覧ください。

3. $g(k)$ について

Waring 問題に限らず、広く整数の加法的理論の研究は、1920 年頃の circle method の誕生を境に一変している。それより前は代数的な手法のみであったが、それ以後は circle method 一色となった、といえるくらいの変わりようである。今回の発表の際には、この circle method の概要についてごく簡単に紹介することも試みたが、ここでは省略させていただき、それについては Vaughan [9] の第 2 章をご参照いただくことにしたい。加えてその本 [9] の第 4, 5, 6 章などをお読みいただくと、Waring 問題への circle method の応用についてかなり詳しくご理解いただけるであろう。

なんにしても、Waring 問題におけるこのような研究の流れを振り返ると、代数的方法がより優れた circle method という解析的な方法に敗れた、というふうにもみえる。少なくとも私は最初そういう印象をもった。が、いろいろと勉強していくうちに、そうではなく、k が大きくなればなるほど解析的な方法が強力になるが、k が小さいうちは代数的な方法が優っている、とみるべきではないか、という気がしてきた。そういう気になっ

---

†言うまでもなく、$k = 2$ のときは上述の平方数の和に関する古典的な結果から、$G(2) = 4$ であることが分かっている。

てきた根拠を伝えるのは難しいと思うが、今では $g(k)$ の決定にまつわる歴史を示せばある程度伝わるのではないか、と考えている。その歴史をみよう。

まず、上述の通り1770年にLagrangeが $g(2)=4$ を示した。1909年になってWieferichが $g(3)=9$ の証明を発表したが、3年後にKempnerがその一部に誤りがあることを指摘し、修正している。いずれにしてもここまでは純粋に代数的な手法による成果である。

その後1920年前後からcircle methodが現れ、それにより前節で述べたように1920年代の半ばには $g(k)$ の決定は原理的には可能となっていた。1936年には7以上の k に対して $g(k)$ は("原理的に"ではなく"実際に")決定された—といっていい状態であったと思う。これは直接にはDickson、Pillai、Nivenらによるが、I.M. Vinogradovの貢献も大きい。ちょっと歯切れの悪い言い方になったのは、そのNivenの論文は1944年のものだからであるが、Dickson、Pillaiの論文はいずれも1936年のもので、例えばDicksonはそのとき $7\leq k\leq 180$ なる k に対して $g(k)$ を決定していて、それをみれば7以上の k が与えられれば $g(k)$ の値を求められますよ、という雰囲気が見えると思うので、上のように表現してみた。

さて残りは $k=4,5,6$ の3つとなったが、1940年にPillaiが $g(6)=73$ を、1964年にChen(陳景潤)が $g(5)=37$ をそれぞれ証明した。最後に残った4乗数の場合については、1980年代の中ごろにBarasubramanian-Deshouillers-Dressが $g(4)=19$ を証明できた、と発表したが、その完全な証明は1988年から1993年にかけて出版されたDeshouillersあるいはDeshouillers-Dressの4編の論文から成る。

まとめると、代数的な方法で $k=2$、3の順番にできたが、4はできなくて、そこにcircle methodが出てきて今度は k が大きい順にできてくるようなことになって、$k=4$ が最後にできた、ということである。これは「k が小さいほど代数的な方法が強く、k が大きいほど解析的な方法が強い、そしてその境目は $k=3$、4のあたりらしい」という印象を与えるもの—といえなくもないであろう。少なくとも私はそういう面もあるな、という感じをもっている。そして、だとすればその境目のあたりでは、代数的な方法と解析的な方法とをうまく融合する、という方針で成果が得られる余地があるかもしれない。一言で言えば、これが私の今回の話の要点である。そのような着想の研究はそれまではなかったといえると思う。

ところで、さっきは7以上の k に対して $g(k)$ がどう決まっているのかについて書かなかったので、気になっている読者もいらっしゃるかもし

れない。話は脇道にそれるが、次節に進む前にここでそれについて書いておこう。いま $A_k = [(3/2)^k]$, $B_k = (3/2)^k - [(3/2)^k]$, $C_k = [(4/3)^k]$ とおけば、実際すべての k について $g(k)$ は次のようになる[‡]。

(i) $A_k + 2^k B_k \le 2^k$ のときは、

$$g(k) = 2^k + [(3/2)^k] - 2.$$

(ii) $A_k + 2^k B_k > 2^k$ かつ $A_k C_k + A_k + C_k = 2^k$ のときは、

$$g(k) = 2^k + [(3/2)^k] + [(4/3)^k] - 2.$$

(iii) $A_k + 2^k B_k > 2^k$ かつ $A_k C_k + A_k + C_k > 2^k$ のときは、

$$g(k) = 2^k + [(3/2)^k] + [(4/3)^k] - 3.$$

すべての自然数 k に対して $A_k C_k + A_k + C_k \ge 2^k$ であることは簡単に分かるから、どの k に対しても必ず上の (i), (ii), (iii) のうちのどれか一つの場合のみが起こる。この意味で $g(k)$ は完全に決定されている。

ただし、すべての k は (i) の条件をみたす、したがって(1) において常に等号が成立する、という予想がある。実際 4 億 7160 万以下の k はすべて (i) の条件をみたす (Kubina-Wunderlich, 1990)。(i) の条件をみたさない k は一つも見つかっていないが、あるとしても高々有限個しかないことを Mahler が 1957 年に示している。しかし Mahler の証明は (i) の条件をみたさない最大の k に対する原理的に計算可能な上界は与えない。いずれにしてもこういう意味では、$g(k)$ にまつわる問題はすべて終わったわけではない、ともいえるわけだが、少なくともそれはもはや加法的整数論の問題ではない。

4. Watson の仕事と恒等式

代数的手法と解析的手法の優劣の境目となっていそうな 3 乗数、4 乗数のあたりで、それらをうまく融合することができないだろうか、という方針を前節で書いた。解析的手法とは、とりあえず circle method を指している。代数的手法としては 1910 年代以前の Waring 問題の研究手段を想定していたが、それを簡潔に述べれば、古典的な平方数の和に関する

[‡] 本当につまらないことだが、形式的に $k = 1$ とすると (i) の場合になり、$g(1) = 1$ となり理に適っている。

結果を基にし、都合のいい恒等式を見つけて議論を組み立てる、というものであったといえると思う。それらを合わせるという方針を思い付いた大きなきっかけとなったのは、次に述べるWatsonの仕事 [14] である。

Wieferichが $g(3)=9$ の証明を発表した直後、その証明は $G(3)\leq 8$ をも示していることをLandauが指摘している。そして1943年にLinnikが $G(3)\leq 7$ を証明した。Linnikのseven cube theoremと呼ばれるこの結果は、$G(3)$ の評価として今でも最良のものである。Watson [14] は1951年、このLinnikの定理に対する簡潔で素晴らしい証明を発表した。これを読んで私はとても感銘を受けたし、こんな仕事をしてみたい、とも思ったものである。その気持ちは今も変わらないし、この論文 [14] は自分の一番大好きな論文だといっていいと思う。このWatsonの議論は、いろんなことが絶妙にバランスをとって成立しているような感があり、ちょっとでもずれると崩れてしまうかのような脆さも感じられたりして、そこがまた素敵なのだ。したがって何の応用もない、ただ $G(3)\leq 7$ を示すためだけの方法といえる。多くの応用があったりする深い、高度な、美しい数学の理論の対極にあるともいえるWatsonの議論であるが、こういうのもまた美しいなあ、と思うのである。Watson [14] のあと、その影響を受けた論文というのはこれまでになかったように思うし、今回報告するWooley氏との共同研究 [4]、[5] も表面的には、あるいは直接的には、Watson [14] と何の関係もないけれども、implicitには影響を受けた仕事である、といっておきたい。

Watson [14] の証明は等差数列中の素数の分布に関する結果も使うから、純粋に代数的なものとはいえないと思うが、その議論の主役となっているのはある特殊な恒等式である。それだけをここに書いても全くしょうがないのだが、敢えて書くと、それはこんなものである。

$$\begin{aligned}(q^6p+r^3x)^3&+(q^6p-r^3x)^3+\\&(q^6p+r^3y)^3+(q^6p-r^3y)^3+(r^6p+q^3z)^3+(r^6p-q^3z)^3\\&\qquad=(4q^{18}+2r^{18})p^3+6q^6r^6p(x^2+y^2+z^2).\end{aligned}$$

なぜ彼はこんな恒等式にたどり着いたのか... これを見れば誰でも知りたくなるのではなかろうか。彼に直接会うことができたなら是非話を聞いてみたい、とも思うが、いややはり自力で読み取るべきだ、とも思っている。まだ完全には分からないのだが、それでも折りに触れ考えているうちに徐々にみえてきているところもある。たぶん $(x+y)^3+(x-y)^3=2x^3+6xy^2$ という恒等式を眺めることから始めて、それをいじりながら上の恒等式

に到達したのではないか—これは多くの方に同意していただける推測ではないだろうか。そこでこのような方針を4乗数に応用するには、まず$(x+y)^4+(x-y)^4$を観察することから始めてみよう、と思ったわけである。といっても正直なところ、うまくいってもせいぜい$g(4)=19$の証明の簡略化といった程度のことしかできないんだろうけど、と思っていた。

ここからの事情については、拙文[2]にも書いた。そこには次節で述べるような結果の証明の概要などについてのより詳しい説明もあるので、お暇と興味のある方は、どうぞ。さて、$(x+y)^3+(x-y)^3$と$(x+y)^4+(x-y)^4$では展開したときの項の数が違うから、状況は全く異なるようである。後者はx^2とy^2の2次形式になるが、とりあえずそれを平方完成してみたら、

$$(x+y)^4+(x-y)^4=2x^4+12x^2y^2+2y^4=2(x^2+3y^2)^2-16y^4$$

となり、

$$(x+y)^4+(x-y)^4+(2y)^4=2(x^2+3y^2)^2 \tag{3}$$

を得た。あっさり見つかったものだが、circle method関連について一通りの知識があると、これは衝撃的である。実際にcircle methodを使う立場でみると、(3)は「平方数は3つの4乗数の和となる」(もちろんこれは正しくない命題だが)というくらいのインパクトのあるものなのだ。

Dicksonの歴史の本[1]の22章の脚注227によると、1878年にProthが恒等式

$$x^4+y^4+(x+y)^4=2(x^2+xy+y^2)^2 \tag{4}$$

を発見した、とされている。$x-y$と$2y$を足すと$x+y$になるから、(3)は(4)と同じことで、それ自身は新しい発見ではなかった。また、Ramanujanの研究で知られるBerndt氏によると、Ramanujanもこの恒等式(4)は知っていて、それをWaring問題の研究に利用する、という着想もRamanujanの手紙の中にあるそうである。Ramanujanはcircle methodの創始に関わった一人であるが、彼がその着想をもったころはまだcircle methodの方が熟しきっていなかった、ということかもしれない— circle method自体やその利用の仕方が今の形にまで簡略にできたのはI.M. Vinogadovの寄与が大きいようだが、今となっては(4)をcircle methodによる議論にのせてWaring問題に応用することは簡単なことである。それによって導かれる帰結のうち、純粋なWaring問題に関係するものを次節に書く。こ

ういう言い方も不適切なのかもしれないが、それらの結果が自分のところに回ってきたのは、いろいろな意味で幸運だったなあ、と思う。

では、もう一つの恒等式の話に触れて、この節を終えることにしよう。2つの恒等式(3)と(4)は同じ、と書いたし、実際そうだが、(4)の形を見て

$$x^2 + y^2 + (x+y)^2 = 2(x^2 + xy + y^2) \tag{5}$$

に気づいた(まあ、気づいた、というほどのことでもないが)。この(5)と(4)の類似はたまたまのこと... であろうが、あとでみるようにこの偶然の類似はそれなりに重要なことであったのである。

5. 4乗数の和に関する成果

この節では、恒等式(4)とcircle methodによって得られる4乗数のWaring問題に関する成果を3つ列挙する。

以下、Xは十分大きい実数とする(例えば$X > 100$くらいでも大丈夫)。X以下の自然数のうち5個の4乗数の和で表せるものの個数を$N(X)$とする。$N(X) < X$は当たり前だが、$X \to \infty$のとき$N(X) \sim X/3$と予想されている。この$N(X)$のような量に対して下からの良い評価を得ること、つまりこの場合で言えば5個の4乗数の和となる自然数が多いということを示すことは、それ自身興味深い問題であるだけでなく、$G(k)$の評価とも関係する大事な課題である。この$N(X)$についても、実際、下からの評価がだんだんと改良されてきた歴史がある。我々の論文[5]の前の最良の結果は、任意に固定した正数εに対して

$$N(X) \gg X^{\theta-\varepsilon}, \qquad ここに\ \theta = (103 - 9\sqrt{5})/88\ (約\ 0.9417)$$

というもので[§]、Vaughan [8]による。

一方、1つの平方数と2つの4乗数の和で表せるX以下の自然数の個数を$M(X)$とすると、任意に固定した正数εに対し、$M(X) \gg X^{1-\varepsilon}$であることが容易に示されることが知られている[¶]。その証明は、平方数のところを$2p^2$の形の数で置き換えても変わらない、さらにそのpを、3を法として1と合同な素数に制限してもほとんど変わらない。つまり、$2p^2+u^4+v^4$ (u, vは自然数、pは3を法として1と合同な素数)の形で表される自然数

[§] $A \ll B$あるいは$B \gg A$は、$A = O(B)$と同じ意味で、ある定数Cがあって$|A| \le CB$ということである。$\ll$や$\gg$はVinogradov symbolと呼ばれる。ここの直前の$N(X)$の評価のような場合、省略されている定数はεに依存し得る。

[¶] Vaughan [9], §2.8, Exercise 6の前半の結果と、§6.1の最初の段落内にあるようなCauchyの不等式の利用により得られる。あるいは[2], pp.160-161を参照されたい。

のうち、X 以下のものの個数を $N_0(X)$ とすると、$M(X)$ のときと同じ証明で $N_0(X) \gg X^{1-\epsilon}$ が従う。ところが、3を法として1と合同な素数 p に対しては $p = x^2 + xy + y^2$ をみたす整数 x、y があるから、(4) により $2p^2$ は3つの4乗数の和で表せることが分かる。すると $N_0(X)$ で数えられる自然数は5個の4乗数の和となることがわかるから $N(X) \geq N_0(X)$ であり、上で Vaughan [8] から引用した $N(X)$ の下からの評価の式において、θ を1にまで大きくできることが分かる。前節で(3)は1つの平方数を3つの4乗数の和に分解するような効果がある、という意味のことを書いたつもりだが、それはこのような状況を言いたかったのである。

ここに書いた議論をもっと精密に行うと、次の結果を得る。

定理 1 (Kawada-Wooley [5], Theorem 1) 任意に固定した正数 ε に対し、

$$N(X) \gg X(\log X)^{-1} \exp\left(-(2+\varepsilon)\sqrt{\log\log X \log\log\log X}\right).$$

この結果は、$N(X) \gg X(\log X)^{-1-\epsilon}$ と書いた方が、少々弱くはなるが、見易いかもしれない。いずれにしてもまだ最終的な結果には遠いが、それにぐっと近づいた、とはいえるのではないかと思う。

次に $G(4)$ に関する話題に移ろう。といっても、実は Davenport が 1939 年に既に $G(4) = 16$ と決定しているのである。これは3以上の k に対する $G(k)$ の予想(2)が解決している、今のところ唯一の場合である。が、それで終わり、ではない。s が16より小さい自然数になると、確かに s 個の4乗数の和で表せない自然数は無限個ある[‖]わけだが、それでもそれらをすべて決定する、ということを目指すべきである。そのために、まず簡単な準備をしておく。

以下、s を16未満の自然数とする。整数 r と法16で合同な自然数全体の集合を $R(r)$ とし、

$$\mathcal{N}_s = \bigcup_{1\leq r\leq s} R(r), \qquad \mathcal{M}_s = \bigcup_{s<r\leq 15} R(r)$$

とする[**]。

さて、整数 x の偶奇によって x^4 は16を法として0か1と合同である。このことから、$\mathcal{M}_s$ に属する自然数は絶対に s 個の4乗数の和とならないことがすぐ分かる。さらに、自然数 n に対して $16n$ が s 個の4乗数の和

[‖]例えば、$16^m \cdot 31$ (m は0以上の整数) の形の自然数はすべて15個 (以下) の4乗数の和で表せないことが初等的な議論で示せる。

[**]もちろん $\mathcal{M}_{15}$ は空集合である。

になったとすると、$s<16$ に注意して、その s 個の4乗数はすべて偶数でなければならないことが分かる。ゆえに n と $16n$ は、両方とも s 個の4乗数の和になるか、両方ともそうでないか、のどちらかであり、よって n と $16^m n$ (m は0以上の整数) でも同様である。したがって、ある16の倍数が s 個の4乗数の和で表せるかどうかを判定するには、それを16で割り切れなくなるまで繰り返し割って得られた数 (それは $\mathcal{N}_s$ か $\mathcal{M}_s$ に属するわけだが) が s 個の4乗数の和で表せるかどうかを判定すればよいわけで、この意味で16の倍数は無視していいのである。

そこで、$\mathcal{N}_s$ に属する自然数のうち s 個の4乗数の和で表せないもの全体の集合を $\mathcal{E}_s$ とすると、上の考察から、s 個の4乗数の和で表せない自然数全体は、無限集合にはなるが、

$$\{16^m \cdot n\,;\, m \geq 0,\ n \in \mathcal{E}_s\} \cup \mathcal{M}_s$$

と表せる。よって、$\mathcal{E}_s$ を決定すれば、s 個の4乗数の和で表せない自然数をすべて決定したことになる。実際 $s \geq 5$ である限りはこの $\mathcal{E}_s$ は有限集合になるだろう、つまり十分大きい $\mathcal{N}_s$ の元は s 個の4乗数の和になるだろう、と予想される。こういう背景があって、$G(4)$ が決定された後は、次のように定義される $G^\sharp(4)$ なるもの[††]を上から評価することが、4乗数の Waring 問題に関して最も興味のもたれる研究課題となったのである。

$G^\sharp(4)$:「$\mathcal{N}_s$ に属する十分大きい自然数はすべて s 個の4乗数の和で表せる」ような s の最小値

Davenport は1939年、$G^\sharp(4) \leq 14$ を証明し、その系として $G(4)=16$ を得たのである。これはわりと長い間改良されなかったが、1980年代の中ごろに Thanigasalam と Vaughan が独立に $G^\sharp(4) \leq 13$ を示した。そして1989年に Vaughan [8] は $G^\sharp(4) \leq 12$ を示し、これが今のところ最良の評価である。この Vaughan の論文 [8] は、その後10年ほどの間に加法的整数論の研究に大きな進展をもたらした、大変重要な仕事である。上記の議論から分かるように、$G^\sharp(4) \leq 12$ が示されたということは、$\mathcal{E}_{12}$ は有限集合で、"原理的には" その元をすべて特定できる、さらに、12個の4乗数の和で表せない自然数をすべてを決定できるということを意味している。

[††] この記号は Vaughan [7] によるが、$G(k)$ ほど広く通用はしていないかもしれない。4乗数の Waring 問題について論文を書いた人は少ない、ということでもあると思うが。

では、我々の恒等式(4) はこの方面に関してどのような帰結をもたらすか、であるが、Vaughan の 12 個を超えて、11 個の 4 乗数の和についてある程度のことはいえるのだが、大変残念ながら $G^\sharp(4) \leq 11$ を証明することはできない。その理由は全く単純なことである。我々の方針は、自然数を 4 乗数の和で表す際、その 4 乗数のうちの 3 つを(4) の左辺の形になるようにする、というものであるが、x、y、$x+y$ の 3 つは、当たり前のことだが、同時に奇数にはなれないから、そうすると 4 乗数のうちの少なくとも一つは偶数でなければならないことになる。しかし上の考察から明らかなように、法 16 で 11 と合同な自然数が 11 個の 4 乗数の和になったとすると、その 4 乗数は全部奇数でなくてはならない。つまり、剰余類 $R(11)$ に属する自然数が 11 個の 4 乗数の和となることを示したければ、あの恒等式(4) を使うことはできないのである。結局、16 個よりも少ない個数の 4 乗数の和に対して恒等式(4) を応用しようと思った瞬間に、法 16 の剰余類 1 つは絶対に手の届かないものになるのである。これはこの方法の致命的な欠陥であり、どうにも避けようがない。

世界新記録 $G^\sharp(4) \leq 11$ には剰余類 1 個分届かなかったが、そのどうしようもない剰余類 $R(11)$ を除いて、11 個の 4 乗数の和について次の結果を得た。

定理 2 (Kawada-Wooley [5], Theorem 3) $\mathcal{N}_{10}$ に属する十分大きい自然数はすべて 11 個の 4 乗数の和で表せる。

上記の通り 16 の倍数は考えなくていいし、$\mathcal{M}_{11}$ の元はみんな 11 個の 4 乗数の和にならないことが分かってるから、くどいようだが、あとは $R(11)$ さえこの定理に加えることができれば良かったのだが... いつかなんとかできたらいいなあ、と思っている。

それでは 4 乗数に関する最後の話題に進もう。前節で書いた通り、初めはこういったことは $g(4)=19$ の証明の簡略化に役立つだろう、と思っていたわけだが、実際その通りであった。

ここで、第 2 節で $g(k)$、$G(k)$ の定義に関連して導入した記号 $s(n,k)$ を再び使いたい。ただここでは 4 乗数の話しかしないから、$s(n)=s(n,4)$ とおこう。つまり、n を 4 乗数の和として表すときに必要な 4 乗数の個数の最小値が $s(n)$ である。$g(4)=19$ を示すには、「$n > C \Rightarrow s(n) \leq 19$」となる C を circle method で具体的に得て、そしてコンピューターでの計算を基に C 以下のすべての自然数 n に対して $s(n) \leq 19$ を確認する、という手順を踏む。Deshouillers-Dress の証明ではこの前半で得られる C の

値は 10^{367} で、後半の確認のためにその当時の大型コンピューターで優に1ヶ月以上は要したようである。恒等式(4)を用いる我々の方法では、前半の circle method で得られる C の値は 10^{146} まで小さくなる。筆者はコンピューターについてあまり良く知らないが、それでも手元のそれほど新しくもないノート型パソコンを2時間ほど使えば、その結果を基に 10^{146} 以下の自然数がすべて高々19個の4乗数の和となることを確認できる。それでも結局コンピューターに依存しているんだから大差ない、という気もするが、circle method に関わる部分も楽になっているし、$g(4)=19$ の証明を結構簡略化したといえると思う。

そして、それ以上のことを示すこともできる。$G(4)=16$ だから16個の4乗数の和で表せない自然数、つまり $s(n)>16$ となる n は、有限個しかないことは分かっていたわけだが、そのような n をすべて決定することができた。この仕事について私が関与した部分は、10^{216} より大きい、16の倍数でない自然数は(ちょうど)16個の4乗数の和で表せる、ということの証明であり、これは Deshouillers-Kawada-Wooley の共同研究である。この論文はもう少しで投稿できる、という段階である。この仕事には(4)だけでなく(5)も重要な役割を果たしているのだが、その辺の事情については、拙文[3]にあるより詳しい解説をご覧いただくこととしたい。また、16個の和の場合でも(4)の形を1回用いると法16の剰余類を1つ失うことにはなるのだが、それは問題ないのである。なぜならば失う剰余類は $R(16)$ で、上で見た通り16の倍数は無視してよかったからである。

コンピューターを用いた 10^{216} 以下の自然数に対するチェックに関する仕事は、Deshouillers-Hennecart-Landreau による。実際彼らは 10^{245} までの自然数 n について、$s(n)>16$ となるものが96個あること、それら以外は $s(n)\leq 16$ をみたすことを確認した。

これらの仕事を合わせて得られる結果をここに記しておく。

定理 3 (Deshouillers-Hennecart-Kawada-Landreau-Wooley) 高々16個の4乗数の和で表せない自然数は全部で96個ある。そのうちの最大数は13792であり、したがってとくに、13793以上の整数はすべて高々16個の4乗数の和で表せる。

$s(n)>16$ となるその96個の n のリストは、例えば[3]にある。$g(4)=19$ ということはすべての n について $s(n)\leq 19$ ということだから、$s(n)>16$ なら $s(n)$ の値はもちろん17か18か19であり、$s(n)=17$、18、19となる n をそれぞれ決定することはもはや簡単な作業である。これらの結果

についても [3] をお読みいただくと分かるようになっている。4 乗数の和で表すとき本当に 19 個必要とする自然数、いいかえれば、18 個以下の 4 乗数の和とならない自然数は 7 個で、書くのも簡単なので、ここではそれだけ紹介しておく。そのような自然数とは即ち $s(n) = 19$ となる n のことだが、

$$s(n) = 19 \iff n = 80m - 1 \ \ (m = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7)$$

である。こんなのを覚えても何の役にもたたないのは明らかだが、害になるわけでもないし、覚えるのも簡単なことだと思うので、せっかくここまでお読みくださった極めて稀なあなたには、是非とも忘れないでいただきたいものである[‡‡]。

6. 5 乗数に関して—結び

加法的整数論の研究において圧倒的な威力を誇る circle method による議論の中に、うまい恒等式を見つけて組み込む、という発想が有効になるとしたら、4 乗数あたりが狙い目なのではないか、と見込んだ理由の一部は第 3 節に書いてみたつもりである。結果として 4 乗数に関しては前節にあるような成果があった。では、他のべき乗はどうだろうか。

次数が小さいほど、解析的手法より代数的手法の方が強くなるようだ、と第 3 節に書いたが、少なくとも $G(k)$ の評価に関して言えば、$k = 3$ までは代数的な手法が強い世界になっているようにみえる。少なくとも Linnik を上回る $G(3) \leq 6$ は、circle method を使っては証明できないだろう。そう思うわけを書くには circle method の議論の概要を書かなければならなくなるから、ここでは止めておきたいが、ある程度の根拠をもってそう言える。これは筆者個人の意見ではなく、この分野の研究者に共通の感想であろうと思う。$G(3) \leq 6$ の証明は、代数的手法が主役となるものだろう、と想像している。

それでは 5 乗数の方はどうだろうか。まずは馬鹿の一つ覚えで、

$$(x+y)^5 + (x-y)^5 = 2x^5 + 20x^3y^2 + 10xy^4$$

を見てみる。右辺は y について偶数次の項しかないから、恒等式(4) と(5) から、

$$\begin{aligned}(x+y)^5 + (x-y)^5 + (x+z)^5 + (x-z)^5 + (x+y+z)^5 + (x-y-z)^5 \\ = 2x(3x^4 + 20x^2(y^2+yz+z^2) + 10(y^2+yz+z^2)^2) \quad (6)\end{aligned}$$

[‡‡] 真に受けないでくださいね。

にたどり着く。右辺は、本質的には1次式と2次式の積に因数分解されているようなことになっていて、これも役に立ちそうな恒等式なのである。

この恒等式(6)とcircle methodを使って$G(5)$の評価をしてみると、比較的楽に$G(5) \leq 21$を証明することができる(Kawada-Wooley [4])。これはThanigasalamとVaughanが1980年代半ばに独立に発表した結果である。ただ(6)を使う証明の方が簡単だし、例えば前節の定理1に対応するような結果で比べれば、我々の方法はThanigasalamやVaughanの成果を上回っている。が、今ではもうVaughan-Wooley [12]が$G(5) \leq 17$を示しているのである。この(6)を使う議論は証明が楽だからある程度の面白味はあると思うが、いかんせん$G(5) \leq 21$では時代遅れである。

加法的整数論にもWaring問題の拡張や変形などのいろいろな問題があるから、実は(6)に基づく議論によって新しい結果を示すこともできるのだが、純粋なWaring問題とは離れるからここでは深入りはしない。そのような考察は、Kawada-Wooley [4]にある。

結局5乗数のWaring問題については、今回テーマとしたような方針で新しい成果を挙げることは、少なくとも今までのところはできなかった。もちろん(6)とは全く別の恒等式が見つかってうまくいく、ということもありうるかもしれない。しかし、個人的な感想にすぎないが、Vaughan-Wooley [12]の17というのは、あまりにも小さい。少なくとも$G(k)$の評価に関する限りは、5乗にして既に解析的方法が強すぎる、という気がしている。特異な恒等式を見つけてどうこうする、という発想が入り込む余地があるのは、3乗、4乗あたりくらいなのかもしれない。

もちろん3乗、4乗のあたりだけでも興味深い問題はたくさんあるし、5乗数についても定理3のような方向の問題もある。恒等式ばっかり探してる、というんではしょうがないと思うが、そういうのも自分の研究の手立てのうちの一つとして大切にしていきたいと思っている。

最後に— こんな拙文でも書くのに思いのほか手間取りまして、締め切りに大きく遅れることとなってしまいました。数理解析研究所の玉川安騎男先生をはじめ、関係された皆様には大変なご迷惑をお掛けすることになりましたことを深くお詫び申し上げながら、筆を置かせていただき

参考文献

[1] L. E. Dickson, "History of the Theory of Numbers, vol. II", Chelsea, New York, 1934.

[2] 川田浩一, Topics in Waring's problem for fourth powers, 数理解析研究所講究録 1091「解析数論と数論諸分野の交流」(1999), 157-171.

[3] 川田浩一, Topics in Waring's problem for fourth powers, II, 数理解析研究所講究録 1160「解析的整数論とその周辺」(2000), 220-228.

[4] K. Kawada and T. D. Wooley, Sums of fifth powers and related topics, Acta Arith. 87 (1998), 27-65.

[5] K. Kawada and T. D. Wooley, Sums of fourth powers and related topics, J. Reine Angew. Math. 512 (1999), 173-223.

[6] M. B. Nathanson, "Additive Number Theory: The Classical Bases." Grad. Text Math. 164, Springer, 1996.

[7] R. C. Vaughan, On Waring's problem for smaller exponents, Proc. London Math. Soc. (3) 52 (1986), 445-463.

[8] R. C. Vaughan, A new iterative method in Waring's problem, Acta Math. 162 (1989), 1-71.

[9] R. C. Vaughan, "The Hardy-Littlewood Method. 2nd ed." Cambridge Univ. Press, 1997.

[10] R. C. Vaughan and T. D. Wooley, Further improvements in Waring's problem, III: eighth powers, Philos. Trans. Roy. Soc. London Ser. A 345 (1993), 385-396.

[11] R. C. Vaughan and T. D. Wooley, Further improvements in Waring's problem, II: sixth powers, Duke Math. J. 76 (1994), 683-710.

[12] R. C. Vaughan and T. D. Wooley, Further improvements in Waring's problem, Acta Math. 174 (1995), 147-240.

[13] R. C. Vaughan and T. D. Wooley, Further improvements in Waring's Problem, IV: higher powers, Acta Arith. 94 (2000), 203-285.

[14] G. L. Watson, A proof of the seven cube theorem, J. London Math. Soc. 26 (1951), 153-156.

[15] T. D. Wooley, New estimates for smooth Weyl sums, J. London Math. Soc. (2) 51 (1995), 1-13.